SECURITY MODULES IN BI SYSTEMS FOR BULGARIAN MUNICIPALITIES

Rosen KIRILOV, Katia STRAHILOVA,
University of National and World Economy (Sofia, Bulgaria)

Bulgaria is a parliamentary republic with local government. The main administrative territorial unit in which local self-government is the municipality. The territory of Bulgaria is divided into 28 districts and 264 municipalities. To improve its activities municipalities must collect, interpret and use data to maximum benefit, and in ensuring maximum security. It is well municipalities to invest in developing business intelligence systems.

In designing the concept of building a business inteligeltni systems for municipal revenue administration, and security modules to them, it is necessary to embed the highest degree of analytical complexity. Such a system would have the following logical architecture (fig. 1):

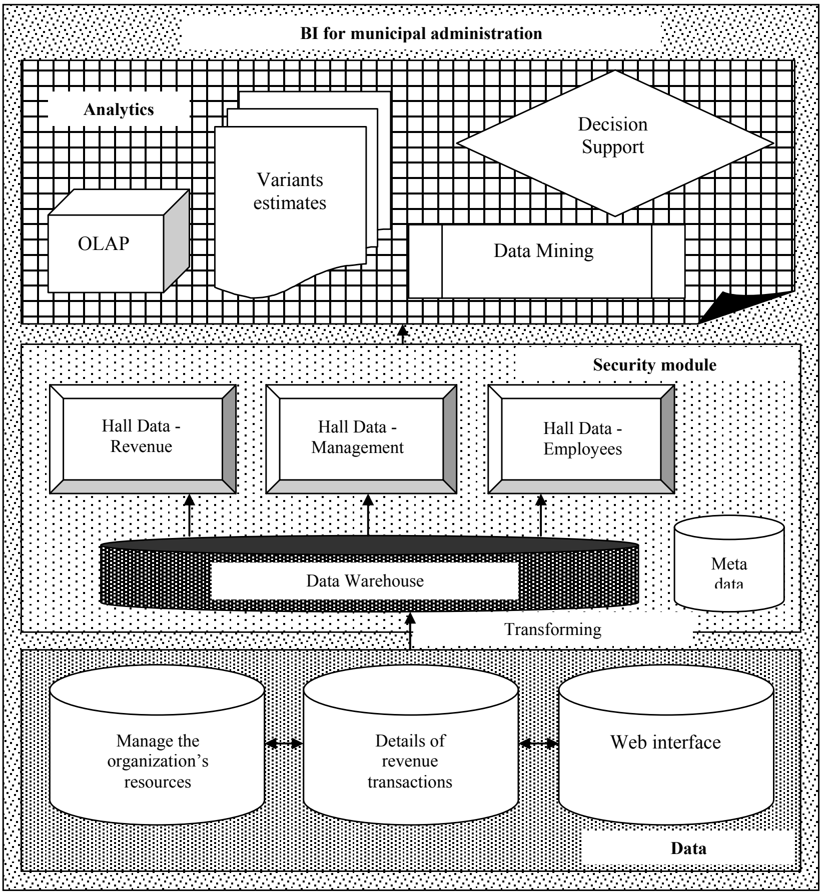

Fig. 1. **BI architecture for municipal administration with security module**

- ***Data Warehouse.*** It is a specialized database or repository of data written to provide job applications to support processes for decision making, ranging from those for regular accounts and inquiries to complex optimization. Data warehouse is constructed with methods, mainly metadata extraction, transformation and loading data;
- The halls are data repositories of information on a specific topic or a specific department (eg property tax);
- ***Business Analytics.*** It provides a large number of software tools that allow users (employees of Revenue Administration) to prepare reports and queries on demand and to analyze the data. They are known as online analytical processing (OLAP). Through these means can be analyzed different dimensions of multidimensional data, time series analysis of trends, ie can quickly and easily identify trends, using a staggered analysis of information and graphics capabilities of products, ensuring the complex data analysis and with integrated capabilities of calculated fields;
- ***Data Mining***. Mining data from a class analysis of information in databases that look for hidden patterns in data group, but can also be used to predict future behavior. It may be developed variants of local budgets. Sometimes the term is misused by connecting only with the possibility of presenting data in new ways, but the real software to extract regularities from the data not only changes the presentation, but really unknown until discovered relationships between data. Subsequently, this knowledge is used in making decisions and achieving certain goals. These instruments are used to reinforce human activity by scanning the large stores of data to detect meaningful new correlations, patterns and trends, using technology to recognize patterns and contemporary statistics;

In this material we define seven principles to consider when developing a strategy for reducing risks to critical information infrastructure:

1. Municipalities should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents.
2. Municipalities should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them.
3. Municipalities should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures.
4. Municipalities should promote partnerships among stakeholders, both public and private, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures.
5. Municipalities should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.
6. Municipalities should ensure that data availability policies take into account the need to protect critical information infrastructures.
7. Municipalities should facilitate tracing attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other municipalities.

The results of the experimental part of this study allow to conclude that municipalities in Bulgaria to comply with laws regarding the budget process and its stages. In this sense, the proposal to build a business intelligence system in a municipal administration would allow much easier budget planning based on operational data. It will also enable the creation of optimistic and pessimistic versions of local budgets, and assist in decision making.

ABOUT CERTAIN VULNERABILITIES OF PSEUDO-M-ROUTERS

Maciej SZMIT
Computer Engineering Department of
Technical University of Lodz (Poland)

This article provides the results of the tests carried out on two models of inexpensive network devices (called „routers", though their functions go beyond the range of the meaning of this term), which are designed for the use in home networks and shows potential dangers which can result from non-standard behaviour of these machines.

Introduction

When the issues regarding network computers are discussed, it is sometimes mentioned about certain incoherency, which takes place between reference model ISO/OSI assumptions and the particular network protocols, and between the network protocols and their specific hardware or software implementations. However, the subject does not attract much attention, especially in the publications on network traffic engineering, which in many cases satisfy themselves with providing information on simplified models[1] and conducting, on their base, computer simulations. Meanwhile, although the ISO/OSI reference model is thirty years old[2], and the basic of the TCP/IP stack protocols came into being more or less at the same time[3], the implementation of the rules and algorithms they provide leave a lot to be desired, causing unforeseen behaviours of their software or hardware. In practical solutions such unforeseen or non-typical behaviour of a specific device can usually lead to its

[1] Model means „simplified reflection of a phenomenon, system, process etc., (. . .), schematic presentation of a fragment of reality, where the insignificant parts are omitted to allow a better explanation of the operation, form or structure of the fragment" [Błaszczuk 2006] s.21. "Model is a depiction of a theory or causal situation, which is assumed to generate the data being observed" [Kendall, Buckland 1986] page 102. "Model (…) is a formal mathematical notation of regularities (…) occurring in the reality" [Witkowska 2005] page 28.

[2] The origin date for the model is considered to be the year 1977, while its present standard was formed in [ISO 7498-1:1994] standard.

[3] [RFC 791] and [RFC 793] are dated 1981